MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2018/2019

TAC3121 – APPLIED CRYPTOGRAPHY

(All sections / Groups)

15 OCTOBER 2018
9 a.m. – 11 a.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 3 pages including the cover page with **FIVE** questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

Question 1

(a) What is a brute force attack? [2 marks]

(b) State Fermat's Theorem, and use it to compute $3^{200} \bmod 7$. [4 marks]

(c) What is a hash function? Define the property of Second Preimage Resistant for a secure hash function. [4 marks]

Question 2

(a) Why must any public key encryption algorithm resist chosen plaintext attack (CPA)? [2 marks]

(b) Construct a Playfair matrix with the keyword "SECRET". Thus, decrypt the ciphertext:

TNDCRCCVCVHEOPDSEKBCUS [5 marks]

(c) Decrypt the ciphertext "RISTVE RGFORE NEATSS" using the row transposition cipher with key sequence: 3 4 1 2 5 6. [3 marks]

Question 3

(a) Can the exponent $e = 2$ be used in RSA? Justify your answer. [2 marks]

(b) Show how Key Generation, Signing and Verification algorithms are performed given the following RSA parameters:

primes, $p = 3$, $q = 11$; exponent, $e = 9$; message, $m = 5$. [5 marks]

(c) Consider a scenario that an adversary Eve has a ciphertext $C = (c_1, c_2) = (g^k, my^k) \bmod p$ encrypted using El Gamal encryption, where g is the generator, m is the plaintext, y is the public key and k is a random number, which she has intercepted from a previous communication between Alice and Bob. Eve will be able to discover the corresponding plaintext of the ciphertext by performing a chosen ciphertext attack. Show the steps involved. [3 marks]

Continued...

Question 4

(a) State the purpose of S-boxes in Data Encryption Standard (DES)? [2 marks]

(b) Given C_5, D_5 as the input key of round 5 in DES. Referring to the schedule of left shifts as shown in Figure 1 below, what is the value of C_5 and D_5 after the key rotation?

$$C_5 = [01101010111100010111000111111]$$
$$D_5 = [11010001000100010001000111111]$$

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure 1. Schedule of Left Shifts

[4 marks]

(c) In Cipher Block Chaining (CBC) mode of DES, if there is a bit error in the plaintext block P_1 during encryption, through how many ciphertext blocks is this error propagated? Justify your answer. [2 marks]

(d) Please state an advantage and a limitation for Counter (CTR) mode. [2 marks]

Question 5

(a) Describe the FOUR (4) adversarial capabilities and the THREE (3) adversarial goals for an encryption scheme. Which combination provides the most desirable security notion? [4 marks]

(b) A digital signature and a message authentication code (MAC) both provide data integrity. What is the additional security goal which can be provided by a digital signature but not by a MAC? Why not? [3 marks]

(c) Diffie-Hellman key exchange is vulnerable to the man-in-the-middle attack. Describe the reason and suggest a solution to overcome this vulnerability. [3 marks]

End of Page